David C. Reymann (8495)
Kade N. Olsen (17775)
PARR BROWN GEE & LOVELESS, P.C.
101 South 200 East, Suite 700
Salt Lake City, UT 84111
(801) 257-7939
dreymann@parrbrown.com
kolsen@parrbrown.com

Steven P. Lehotsky*
Scott A. Keller*
Jeremy Evan Maltz*
LEHOTSKY KELLER COHN LLP
200 Massachusetts Avenue, NW
Washington, DC 20001
(512) 693-8350
steve@lkcfirm.com
scott@lkcfirm.com
jeremy@lkcfirm.com
*(motions for admission pro hac vice forthcoming)

Todd Disher*
Joshua P. Morrow*
Alexis Swartz*
LEHOTSKY KELLER COHN LLP
408 W. 11th Street, 5th Floor
Austin, TX 78701
(512) 693-8350
todd@lkcfirm.com
josh@lkcfirm.com
alexis@lkcfirm.com

Attorneys for Plaintiff NetChoice, LLC

IN THE UNITED STATES DISTRICT COURT
DISTRICT OF UTAH

NETCHOICE, LLC, **Plaintiff,** **v.** **SEAN D. REYES, in his official capacity as Attorney General of Utah,** **KATHERINE HASS, in her official capacity as Director of the Division of Consumer Protection of the Utah Department of Commerce,** **Defendants.**	**DECLARATION OF STACIE D. RUMENAP IN SUPPORT OF PLAINTIFF'S MOTION FOR A PRELIMINARY INJUNCTION** **Case No. _____**

1. ***Identity of Declarant***. I am the President of Stop Child Predators (SCP), a 501(c)(3) nonprofit organization founded in 2005 to combat the sexual exploitation of children and protect the rights of crime victims nationwide. I have led SCP since 2006, having worked in all 50 states—including spearheading the passage of Jessica's Law in 46 states. SCP brings together policy experts, law enforcement officers, community leaders, and parents to launch state and federal campaigns to inform lawmakers and the public about policy changes that will protect America's children from sexual predators both online and in the real world. I make this declaration from personal knowledge.

2. ***SCP's Mission***. SCP works with parents, lawmakers, and policy experts to better educate families, schools, and lawmakers about the potential risks children face both in the real world and online, including grooming, luring, bullying, Child Sexual Abuse Material (CSAM), and other harms to children. SCP has worked for nearly two decades to open lines of dialogue with lawmakers and technology company stakeholders, to help them determine the best and most practical ways to protect children from these risks.

3. SCP focuses significant policy efforts on keeping social media, and the internet more broadly, safe for children. In 2008, we launched the Stop Internet Predators (SIP) initiative in recognition that child predators often use social-networking platforms to recruit child sex-trafficking victims, to groom children for sexual exploitation, and to sexually victimize children in general, and sex offender management, and that child safety must therefore be addressed both in the real world and online. Our more recent Digital Safety Project adapts the SIP initiative's goals to a new online landscape and operates from the premise that the private sector plays an important role in protecting children. Through this project, we also work to ensure that the government doesn't unnecessarily interfere with the protection of children or the ability of parents to decide what's best for their children.

4. We believe that the internet and social media have incalculable value for our young

people—particularly those who are disabled, suffer from anxiety, or are in other circumstances that make it difficult for them to connect in person. We, therefore, work with leading online services, including some of Plaintiff's members, to develop and enforce policies that prioritize children's safety while still promoting free speech and ensuring children have access to valuable technology. Our goal is to help businesses develop tools and mechanisms to identify and promptly take down illegal content (CSAM), and to help them identify products and services that may be used by predators to target and lure children. These tools and mechanisms help businesses mitigate the potential for their products and services to be used to cause harm.

5. ***The Social Media Regulation Act.*** We are concerned that The Social Media Regulation Act, while ostensibly intended to make the internet safer for children, will instead result in serious negative outcomes for children. The law mandates that companies cannot collect a minor's data.[1] We are concerned about this provision. In cases where a child is a victim of kidnapping or another crime, data - specifically activity logs and change logs – can be useful to law-enforcement and potentially lifesaving to the child. Social media companies are mandated by federal law to cooperate with law enforcement and have been an indispensable resource. For example, last year tech and social media companies provided 99% of all reports to the National Center for Missing and Exploited Children's Cypertipline.[2] In fact, there are so many reports of child exploitation that FBI and Department of Justice officials said that investigating them would require assigning cases to every FBI agent. The government does not presently have the resources to do that.[3] The government's limited resources underscore the importance of private moderation and filtering technologies. In order to detect CSAM, as well as to report it to authorities, online companies can (and must) develop and use advanced algorithms and other screening tools.

6. For example, consider a child unknowingly involved in an online exchange with an

---

[1] https://socialmedia.utah.gov/

[2] https://www.missingkids.org/cybertiplinedata

[3] Katie Benner & Mike Isaac, *Child-Welfare Activists Attack Facebook Over Encryption Plans,* N.Y. Times (Feb. 5, 2020), https://nyti.ms/38rN3IX

older predator, who is masquerading as a young person and attempting to lure the child into a dangerous situation. If the child is ultimately entrapped, their online activity (including their conversations with the predator and their search history) could be critically helpful in finding the child, but if sites are prevented from collecting this information in the first place, this valuable evidence will be lost. In fact, a child's online activity could reveal patterns that could help private companies alert the children and their parents to something amiss, but those patterns will not come to light if they are erased before they can be analyzed. To provide an example: A child searching for information about bus routes may not be a concern on its own, but a child searching for information about bus routes immediately *after* interacting online with an adult in another state could identify a risk.

7. We are also concerned about The Act's requirement that covered businesses "verify the age of a Utah adult seeking to maintain or open a social media account" and "get the consent of a parent or guardian for Utah users under age 18.[4]" This would require businesses to collect personal information, creating a trove of sensitive data. We consider it not a risk but an inevitability, given the realities of data security, that one or more of these data sets will be breached, exposing the personal information of children as well as adults to bad actors. States, including Utah, are vulnerable to cyberthreats. This past summer's massive data breach at the University of Utah in which the names, addresses, birthdates, social security numbers, and other personal identifying information of thousands of current and former employees and students were exposed is just one example.[5]

8. Additionally, in my work to make the internet safer for children, I have become familiar with the types of technology that companies have considered to verify the ages of their users. I understand that this technology raises accessibility concerns. For instance, a technology

---

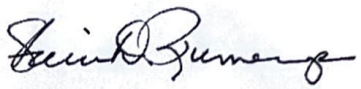
[4] https://socialmedia.utah.gov/

[5] Matt Gephardt & Sloan Schrage. *A massive, global cyberattack has reached Utah, so how can you protect your identity?*. KSL-TV, (July 19, 2023). https://www.ksl.com/article/50689271/a-massive-global-cyberattack-has-reached-utah-so-how-can-you-protect-your-identity

that requires a user to take a photograph of their own face would not be accessible to a person who does not have an integrated camera on their device and may prove practically inaccessible to someone who is vision impaired and cannot easily take a photograph. While we believe the government has an interest in protecting children, we are opposed to a solution that would render portions of the internet inaccessible to disabled and under-resourced individuals.

9. The Act imposes a restriction on social media access for minors by requiring businesses to implement a default curfew, blocking access to minor accounts from 10:30 p.m. to 6:30 a.m. Parents have the option to modify this setting. However, this raises concerns for those minors in abusive or neglectful situations. For these individuals, the internet often serves as a critical resource for assistance in dealing with abuse, substance addiction in the family, and for accessing confidential health services. By creating this barrier, the Act potentially hinders the ability of vulnerable minors to seek help discreetly. Furthermore, it might inadvertently push them towards smaller, less regulated online services, as opposed to larger, more secure ones like Meta or Google, which have invested significantly in user protections.

I, Stacie D. Rumenap, declare under penalty of perjury under the laws of the United States of America, pursuant to 28 U.S.C. § 1746, that the foregoing to be true and correct to the best of my knowledge. Executed on this December 15, 2023 in Washington, DC.



Stacie D. Rumenap